HIERARCHICAL OPTICAL VPNs IN A CARRIER'S CARRIER VPN ENVIRONMENT

RELATED U.S. APPLICATION DATA

[0001] Provisional application No. 60/396,899 filed on July 17, 2002.

FIELD OF THE INVENTION

[0002] The present invention relates to hierarchical optical VPNs (Virtual Private Networks) in a carrier's carrier VPN environment and is particularly concerned with allowing subscribers to an optical VPN service to provide optical VPN service to their customers.

BACKGROUND OF THE INVENTION

[0003] A Virtual Private Network (VPN) may be thought of as a private network constructed within a public network infrastructure. Many definitions of VPNs can be considered:

[0004] Definition 1: A VPN is a set of users (devices attached to the network) sharing common membership information and intended to establish inter-site connectivity (within that group). A user can be a member of multiple groups (VPNs).

[0005] Definition 2: A VPN is a client private network that subscribes to restricted connectivity services.

[0006] Definition 3: A VPN is a service where a customer requests multi-site connectivity services provided through a shared network infrastructure.

[0007] Definition 4: A VPN is a service where a partition of internal provider network resources is allocated to a customer.

[0008] An Optical VPN (OVPN) may be considered a VPN including SONET/SDH technologies whose basic unit of service is an optical/TDM physical connection between two endpoints or sites.

[0009] In the network, carriers provide services to subscribers and, in turn, may be subscribers to other carriers' services. A carrier's carrier OVPN service is an Optical VPN service provided by a first carrier itself subscribing to an OVPN service from another second carrier. The carrier's carrier OVPN customer may decide to use its service to provide OVPN services or alternatively may decide to buy directly from the provider OVPN services to be used by his customers.

[0010] In the case where the customer does not or cannot manage the OPVN implementation and decides to outsource it to the provider, the provider will have to restrict connectivity for the client's client OVPNs in order to implement the OVPNs. This may be accomplished either directly through explicit intervention or indirectly by offering the customer the tools to manage its client while still reinforcing the OVPN architecture at the control plane.

[0011] Therefore, what is required is a scalable method or system which would allow the provider to support the customer's multiple OVPNs yet afford aspects such as simplified provisioning, overlapping addresses, constrained/restricted connectivity, on demand bandwidth requests, privacy/independence with respect to addressing and routing, and in general provide VPN services while achieving optical network efficiency and scalability.

SUMMARY OF THE INVENTION

[0012] An object of the present invention is to provide an improved VPN in a carrier's carrier network.

[0013] According to a first aspect of the invention, there is disclosed a network having a set of elements interconnected by services; with at least one first subset of the elements defining a private network and at least one second subset of elements

different from the first subset defining a provider network wherein at least two subgroups of the first subset of elements may be connected via the provider network. The network further has a services hierarchy wherein virtual private networks are defined on the second subset of elements. The services hierarchy includes a "father" virtual private network (VPN) and at least one affiliated "son" VPN. Each son VPN has at most one affiliated father VPN. Each father VPN is responsible for associating services and connections for the at least one affiliated son VPN and the provider network has a means for associating elements forming the father VPN.

[0014] According to another aspect of the invention, there is disclosed a method of organizing a network having a set of elements interconnected by services, wherein at least one first subset of the elements defining a private network and at least one second subset of elements different from the first subset defining a provider network wherein at least two subgroups of the first subset of elements may be connected via the provider network. The method includes establishing a services hierarchy wherein virtual private networks are defined on the second subset of elements. Further, there is established within the services hierarchy a father virtual private network (VPN) and at least one affiliated son VPN wherein each son VPN has at most one affiliated father VPN. Yet further, each father virtual private network is responsible for associating services and connections for the at least one affiliated son VPN; and providing a function for provider network associating elements comprising the father virtual private network.

[0015] Conveniently, the associating function for the provider network includes a VPN descriptor for each father VPN and each son VPN.

[0016] Advantageously, the associating function for the provider network may construct the VPN descriptors using an auto-discovery process.

[0017] The present invention will now be described in more detail with reference to exemplary embodiments thereof as shown in the appended drawings. While the present invention is described below with reference to the preferred embodiments, it should be understood that the present invention is not limited thereto. Those of ordinary skill in the art having access to the teachings herein will recognise additional implementations, modifications, and embodiments which are within the scope of the present invention as disclosed and claimed herein.

BRIEF DESCRIPTION OF THE DRAWINGS

[0018] The invention will be further understood from the following detailed description of embodiments of the invention and accompanying drawings, in which:

[0019] **FIG. 1** is a diagram of a network reference model.

[0020] **FIG. 2** is a diagram of an example carrier's carrier network.

[0021] **FIG. 3** is a diagram of a carrier's carrier model Service Tree.

[0022] **FIG. 4** is a diagram of an example Hierarchical Optical VPN Service Tree according to an embodiment of the invention.

[0023] **FIG. 5** is a diagram of another example Hierarchical Optical VPN Service Tree according to an embodiment of the invention.

[0024] **FIG. 6** is a diagram of an example Hierarchical Optical VPN according to an embodiment of the invention.

[0025] **FIG. 7** is a diagram of an example Partition-based Hierarchical Optical VPN according to an embodiment of the invention.

[0026] **FIG. 8** is a diagram of an example Hierarchical Optical VPN where the provider is managing a customer's OVPNs according to an embodiment of the invention.

[0027] **FIG. 9** is a diagram of a HOVPN Service Tree with inactive levels according to an embodiment of the invention.

[0028] **FIG. 10** is a diagram of a Service Tree showing possible operations according to an embodiment of the invention.

[0029] **FIG. 11** is a diagram of the hierarchical relation of PITs (Port Information Table) in an HPIT (PIT Hierarchy Tree) according to an embodiment of the invention.

[0030] **FIG. 12** is a diagram of an example HPIT Tree according to an embodiment of the invention.

[0031] **FIG. 13** is a diagram of a HOVPN Policy Tree according to an embodiment of the invention.

[0032] **FIG. 14** is a diagram of a GIT (Globally Unique Identifier Table) according to an embodiment of the invention.

[0033] **FIG. 15** is an illustration of signaling used to establish connectively for a HOVPN according to an embodiment of the invention.

[0034] **FIG. 16** is a diagram of a signal traversing a Service Tree according to an embodiment of the invention.

[0035] **FIG. 17** is a diagram of a signal traversing a Service Tree and leaving a defined partition according to an embodiment of the invention.

[0036] **FIG. 18** is a diagram of a service scenario with Auto-Discovery according to an embodiment of the invention.

[0037] **FIG. 19** is a diagram of a service scenario showing a connection according to an embodiment of the invention.

DETAILED DESCRIPTION

[0038] Referring to **FIG. 1**, there is illustrated a network having a Service Provider portion **100** with customer networks **110** connected to it. The Provider's network has network elements **115** and the portion of the Provider's network that interfaces with a particular customer network is a Provider Edge (PE) device **120**. The portion of the customer's network which interfaces to the PE device **120** is a Customer Edge (CE) device **125**. In this context, services means at least signalling or connectivity services.

[0039] Referring to **FIG. 2**, there may be seen an illustration of an example carrier's carrier model service scenario. In this example, Client 1 **131** and Client 2 **132** each subscribes to a port-based Optical VPN from Provider A **140**.

[0040] CLIENT 1 **131** provides optical VPNs to Client 3 **133** and Client 4 **134** on the same Optical VPN (OVPN) bought by CLIENT 1 **131**. CLIENT 1 **131** may decide that it would be preferable for Provider A **140** to provide all the OVPN functionality for CLIENT 1 **131** OVPN customers.

[0041] In terms of addressing, CLIENT 1 **131** may wish to use its own private addressing or use provider public addresses. CLIENT 3 **133** and Client 4 **134** may wish to use CLIENT 1 **131** addresses or addresses provided by Provider A **140**.

[0042] **FIG. 3** is an alternative depiction of a portion of the service arrangement of **FIG. 2** in the form of a service tree. It may be seen that Provider A **140** supplies services to CLIENT 1 **131** who in turn provides services to Client 3 **133** and Client 4 **134**.

[0043] A carrier's carrier OVPN service is an Optical VPN service provided by a carrier itself subscribing to an OVPN service from another carrier. An example would be Client 1 **131** who is providing service to Client 3 **133** while in turn subscribing to service from Provider A **140**.

[0044] Hierarchical Optical Virtual Private N tworks (HOVPNs)

[0045] A Hierarchical Optical VPN (HOVPN) is an OVPN service associated with a hierarchical service tree. A hierarchical service tree is a tree of Optical VPN services involved in a hierarchy relationship.

[0046] A Hierarchical Port-based OVPN is a hierarchy of port-based OVPN where a father VPN may have one or more son VPNs. A given port may belong at most to one father OVPN.

[0047] Connections can be triggered by any son VPN within the father VPN and so on. On a given father port, multiple OVPN son memberships can be defined. The father port can only belong at most to one OVPN (including the extranet case). It is the role of the father VPN to associate at a given time the channel or connection to the son VPN.

[0048] **FIG. 4** illustrates a hierarchical service tree for the example network previously described. From the service tree Provider **140** provides services to father VPN **131** which services son VPN **133**. In turn, son VPN **133** is father VPN to son VPN **134**. For this service tree, the HOVPN father would be father VPN **131**.

[0049] A Hierarchical Port/Partition-based OVPN is a hierarchy of a mixture of a partition and port-based OVPNs. In this context, a partition is a subgroup of services obtained from a Service Provider which would allow connectivity across the Provider network via the subgroup. **FIG. 5** illustrates an example service tree containing both port-based OVPNs **144** and partition-based OVPNs **145**. This particular tree illustrates an example case where a customer who subscribes to a partition-based VPSTN (Virtual Private Switched Transport Network, a type of partition-based service) decides to use this service to provide both GVPN (Generalized VPN, a port-based VPN service) and VPSTN services to its clients.

[0050] A Hierarchical Port-based OVPN may be considered a hierarchy of port-based OVPN where a father VPN may have one or more son VPNs. A given

port may belong at most to one father OVPN. A Hierarchical Port/Partitionbased OVPN is a hierarchy of a mixture of a partition and port-based OVPNs. Connections can be triggered by any son VPN within the father VPN. On a given father port multiple OVPN son memberships or affiliation may be defined. The father port can only belong at most to one OVPN (including the extranet case). It is the role of the father VPN to associate at a given time the channel/connection to the son OVPN. **FIG. 6** illustrates an example HOVPN network according to this arrangement with Service Provider **140**, father OVPN **147** and son OVPN **148**. Note that several of the VPNs are connected via networks **150** which may be Metro networks, for example. The other VPNs **141**, **142**, and **143** which are part of the HOVPN network may also be seen.

[0051] Referring to **FIG. 7**, there is illustrated a Partition-based HOVPN wherein may be seen the partition owned by the customer OVPN-1 **152**, the open partition **153**, *i.e.,* the Provider's network that is not part of the partition **152**, and the connection **154** used for OVPN-User 1 through the partition OVPN-1 **152**.

[0051] Referring to **FIG. 8**, there may be seen an HOVPN example of where the Provider is managing the customer's OVPNs. At PE **160**, there is maintained a service tree of the services provided. The corresponding CE **162** may be seen as well as the father OVPN1 Control Channel **164**. All the son VPN signalling information will traverse the father control channel.

[0052] For Port-based VPN, a given CE-USER can use the same port as the father OVPN (including the case where all the channels for the father OVPN port are all used by the OVPN "sons"). For Partition-based OVPN, the partition-based port can be used by multiple port-based OVPNs. On a given OVPN father port, multiple OVPN "son" memberships can be defined.

[0053] A given client or provider port may be assigned exclusively to one OVPN at any level within the hierarchy. It is apparent that being able to assign a given port to any level may result in inactive VPNs at levels in the hierarchy. **FIG. 9**

illustrates the service tree for this case where in-use VPNs **164** are hierarchically connected to inactive VPNs **165**.

[0054] Referring to **FIG. 10**, it is apparent that certain operations may be performed on the service tree of an HOVPN which will change the network yet also preserve the hierarchical arrangement. Nodes in the service tree may be added, removed, promoted to a level-n, or demoted to a level-n with associated implications on VPN ownership and management.

[0055] **Building Blocks of an HOVPN**

[0056] **OVPN Descriptor**: *contains information about each Optical VPN (part of an HOVPN).*

[0057] **Port Information Table (PIT):** contains a list of Customer Port Identifier (CPI) and Provider Port Identifier (PPI) tuples for all the ports within an OVPN

[0058] **PIT Hierarchy Tree (HPIT)**: contains a tree of HOVPNs composed of OVPN descriptors at different levels of a hierarchy

[0059] **Global Unique Identifier (GID):** One or more (VPN-IDs, Route Targets, etc.,) and can be allocated per OVPN basis.

[0060] **GID Table (GIT):** holds for each GID the correspondent OVPN descriptor information with its associated level.

[0061] In operation, each carrier's carrier OVPN when configured (*i.e.*, a PIT is added and a port is allocated if it is a port-based OVPN) will be assigned a GID value unique across all OVPNs.

[0062] **Details of an OVPN Descriptor on a Provider Edge**

[0063] An OVPN descriptor ("OVPN Desc") is associated with each Optical VPN service configured on the PE. The OVPN Desc contains (*N.B.*: see Glossary for terms used in the examples below):

- The type of the OVPN service which can have one of the following values: GVPN_c=1, VPOXC_c=2, VPSTN_c=3, UNI based OVPN=4, others types may be defined later, for example, another flavour of port-based OVPNs.
- OVPN Category=port-based, partition-based.
- At least one GID associated with the OVPN. The same GID can be used for the same OVPN configured on multiple PEs.
- Administrative Status value which can be set to "up", "down", or "testing".
- Operational Status value which can be set to "enabled" or "disabled".
- a Port Information Table (PIT): A PIT can be used with services like VPOXC and GVPN (VPSTN only when private routing is not used). A PIT will contain the following information:
    - a Customer Port Identifier (CPI);
    - a Provider Port Identifier (PPI);
    - Channel Characteristics; and
    - Local/AD constants: "AD" is CPI learned from auto-discovery, "Local" means learned from attached CE.

[0064] Example of OVPN Descriptor

- GID=1234567
- OVPN_Type=GVPN
- OVPN_Category=Port_based
- AdminStatus=Up
- OperStatus=enabled

- PIT={<10.1.1.1,16.1.1.1, info1, local>, <10.1.1.2, 16.1.1.2, info2, "AD">,...}.

[0065] **Combining OVPN Descriptors into a PIT Hierarchy Tree (HPIT)**

[0066] For each HOVPN is associated a hierarchical Port Information Table Tree (HPIT Tree). An example HPIT Tree is given in **FIG. 11**. An HPIT is hierarchical ordering of OVPN Descriptors.

[0067] Referring to **FIG. 11**, a customer at level "0" (root of the HPIT tree) subscribes to a direct OVPN service. Therefore a PIT at the root of HPIT is considered the RPIT (Root Port Information Table). A Customer at level 2 subscribes to an OVPN service from an OVPN customer at level-1. A customer at level-n subscribes to an OVPN service at level (n-m where $m \leq n-1$). **FIG. 12** depicts a populated HPIT Tree according to an example embodiment.

[0068] Referring to **FIG. 13** it is apparent that the hierarchical nature allows for topology policies to be defined within each subhierarchy as connectivity is achieved through the hierarchy.

[0069] **HPIT Rules**

[0070] An OVPN service at level-n with a type=VPSTN can provide OVPN services at level (n+m where m=1,...k) of types VPSTN, VPOXC, GVPN and port-based UNI based OVPN.

[0071] An OVPN service at level-n with a type=port-based (GVPN) can only provide OVPN services at level (n+1, n+2, ..., n+m) of type GVPN and UNI based OVPN.

[0072] An HPIT is associated with a list of import/export route targets taken from the list of route targets configured for each individual PIT.

[0073] A given CPI can be used by multiple OVPNs clients of the OVPN where the CPI belongs to. This CPI will be tagged with a list of export route targets coming from the sum of the list of route targets of each PIT where the CPI appears.

[0074] Since addressing is associated with ports on the provider edge, the network allows a VPN at level (n+m where 0 < m) to use the same addressing defined by VPN at level-n. A private address at level-n is considered a public address at level ("n+1"..."n+m").

[0075] According to another contemplated embodiment, another approach would be to allow each OVPN at each level to define and use its own addressing.

[0076] Note that this solution can be applicable to a network environment where public addresses are used at the root VPNs (an example protocol of which would be TNA (Transport Network Assigned Address) as in Optical Internetworking Forum UNi1.0 protocol).

[0077] **Globally Unique Identifiers (GIDs)**

[0078] Globally Unique Identifiers may be used in combination with HOVPNs to allow for auto-discovery mechanisms. The GID may include as well standard-based VPN-ID format as defined in the RFC2685 "Virtual Private Networks Identifier" B. Fox, B. Gleeson; September 1999,

[0079] An HOVPN may own multiple GIDs and multiple GIDs may represent the same HOVPN. The GIDs are used in the control plane to control the VPN membership of the connectivity service.

[0080] **Example GID Format**

[0081] Each GID is encoded as an eight-octet quantity:

[0082] Type Field : 1 or 2 octets

[0083] Value Field : Remaining octets

[0084] **Type Field**: The value of the high-order octet will determine if it is a regular type or extended type:

[0085] Type Field for regular types is 1 octet.

[0086] Type Field for extended types is 2 octets

[0087] The high-order octet of the Type Field is:

[0088] First bit (MSB) : IANA authority bit Value 0.
IANA assignable type Value 1

[0089] Second bit: Vendor-specific types.

[0090] Reserved Remaining 6 bits : Indicates the structure of the GID:

[0091] **Value Field**

[0092] The encoding of the Value Field dependents on the "type" of the GID as specified by the Type Field.

[0093] Four types defined.

[0094] **Type 0x00**: This is an extended type.

[0095] Administrator subfield: 2 octets, contains AS number

[0096] Assigned Number subfield: 4 octets, contains a number from a numbering space which is administered by the enterprise to which the ASN has been assigned by an appropriate authority.

[0097] **Type 0x01**: This is an extended type.

[0098] Administrator subfield: 4 octets, IP address

[0100] Assigned Number subfield: 2 octets, contains a number from a numbering space which is administered by the enterprise to which the IP address has been assigned.

[0101] **Type 0x02**: This is an extended type

[0102] Administrator subfield: 4 octets, contains AS number.

[0103] Assigned Number subfield: 2 octets, contains a number from a numbering space which is administered by the enterprise to which the IP address has been assigned.

[0104] **Type 0x04**: This is a regular type with a type field of 1 octet and a Value Field of 7 octets. The Value Field consists of two subfields:

[0105] Administrator subfield: 3 octets, contains a 3-octet Organizationally Unique Identifier, as defined by ANSI/IEEE. Assignment of OUIs is carried out by the IEEE OUI Registry.

[0106] Assigned Number subfield: 4 octets, the Assigned Number subfield contains a number from a numbering space which is administered by the enterprise to which the OUI has been assigned.

[0107] **GIT Table**

[0108] The GIT table is a table that holds the value of the Global Unique identifiers (GIDs) and their respective PIT (RPIT/HPIT). A GID table is indexed by HPIT levels. **FIG. 14** depicts an unpopulated GIT Table.

[0109] Each HOVPN will be associated with:

- an HPIT Tree;
- a GIT Table; and
- an OVPN Descriptor associated with the HOVPN.

[0110] **Signalling**

[0111] A customer of VPN at level (n+m) can signal optical connection requests provided by VPN service at level-n. For example, a VPN service at level-n is a VPSTN which can provide port-based Optical VPN at level (n+m), even if there is no connection used for OVPN at level ("n+1"..."n+m-1") as per the previous discussion of inactive nodes.

[0112] There is the ability to signal a connection for VPN at level (n+m) using the VPN service provided at level-n.

[0113] For each VPN at level ("n+m", m=1,...k), the connection request will carry the following items:

[0114] source_address (I), I=n,..,n+m can be any address (private used by OVPN at level

[0115] destination_address(I),

[0116] Optionaly GID(n)> where I = 0, ..., n.

[0117] Should a GID not be specified in the connection request, the Root PIT will be used.

[0118] GMPLS based signaling may used (*e.g.*, IETF-GMPLS, OIF-UNI1.0) although the solution described applies in general to any signaling protocol.

[0119] **Connectivity Algorithm**

[0120] Following is the algorithm used to establish connectivity. Referring to **FIG. 15**:

[0121] 1. At a PE1, a connection request **192** occurs with a GID as parameter.

[0122] 2. Using the GID as a reference, obtains both the OVPN descriptor and the level of the OVPN (for example, level-n) from the GIT.

[0123] 3. Ascertains the context of the customer as level-n using the level from the GIT and obtains the associated PPI by consulting the PIT(n) and checking the destination CPI. Formulates a connection request **194** between PEs using associated PPIs.

[0124] 4. At PE2 formulates a connection request **196** completing the overall connection.

[0125] If no GID is present in original connection request **192**, the connection is either for the root VPN or, alternatively, the connection is already set for a given port-based VPN within a given hierarchy (*e.g.*, port-3 is associated with customer at level 3).

[0126] If there is no GIT table the call is cleared.

[0127] **Signalling Traversing the Service Tree**

[0128] Referring to **FIG. 16**, connectivity signaling can traverse multiple OVPNs within the service tree. For example, GVPN-3 **180** may signal connectivity that traverses GVPN-2 **182**, VPSTN1-1 **184**, and root VPSTN-0-1 **186**.

[0129] Referring to **FIG. 17**, when the same port is used for an HOVPN and other OVPNs (that include HOVPNs), then the customer can indicate through the use of GIDs what path the connection should take under various scenarios: the hierarchical tree path **188** or, alternatively, the open-area path **189**. The latter case may be chosen in the case of a link failure on the partition, for example, allowing service to be maintained over the open network until the partition can be restored.

[0130] **Auto-Discovery Mechanism**

[0131] We may define a BGP-based auto-discovery mechanism that allows Client Devices (CDs) which are members of the same VPN to discover each other

and request CD-to-CD optical connections across a service provider optical infrastructure. Note that the VPN auto-discovery mechanism is not limited to one based on BGP but that any suitable VPN auto-discovery mechanism may be used.

[0132] An Optical VPN (OVPN) is defined as a collection of ports that connect the Client Devices owned by the same organization to the service provider network.

[0133] A given service provider network may support multiple OVPNs.

[0134] A port may be considered as a collection of channels, for example, a lightpath, or a SDH/SONET circuit. Not all ports on a given Provider Edge Optical Network Element (PE-ONE) connecting that PE-ONE to Client Devices must belong to the same OVPN.

[0135] An important aspect is the support of single ended provisioning. It is possible to reconfigure an OVPN (*e.g.*, when a Client Device request to set-up a new optical channel trail to another Client Device within the same VPN) without requiring configuration changes in any of the provider's ONEs.

[0136] Within a given OVPN, each port has an identifier unique only within that OVPN called the Customer Port Identifier (CPI). Within a service provider network, each port on a PE-ONE has an identifier that is unique within that service provider network. We refer to this identifier as Provider Port Identifier (PPI). Each PE-ONE maintains a Port Information Table (PIT) for each OVPN that has at least one port on that Provider Edge ONE. A PIT contains a list of <CPI, PPI> tuples for all the ports within its OVPN.

[0137] A PIT on a given PE-ONE is populated from two sources: the information received from the CDs attached to the ports on that PE-ONE, and the information received from other PE-ONEs (received, for example, through BGP).

[0138] Since the protocol used to populate a PIT with remote information is BGP and since GMPLS signaling is not restricted to a single routing domain, it is

contemplated that this mechanism could support an environment consisting of multiple routing domains.

[0139] Referring to **FIG. 18**, an HPIT **200** is created for each HOVPN via VPN Auto-discovery **205**. An example PIT **210** for PE1 illustrates the association of the CPI **212** and the PPI **214** as well as additional information **216**.

[0140] Referring to **FIG. 19**, a depiction of a connection across the network may be seen. The process initiates with a connection request **220** with the following criteria:

[0141] Connection request:

Source address=10.1.1.1,

Destination address=10.1.1.3

GID=45678

[0142] Recourse is made to the GIT **222** for determination of the OVPN descriptor (the example GIT is reproduced in more detail at **223**). The OVPN descriptor allows recourse to VPN-A PIT on PE 1 at level-16 **224** for access of the tuple containing the relevant destination address in the provider network associated with the client destination address (the example VPN-A PIT is reproduced in more detail at **225**). Accordingly, a connection request traversing the provider network using the PPI addresses is generated at **226** as:

[0143] Connection request:

Source address=16.1.1.1,

Destination address=16.1.1.3

[0144] The PE3 element receiving the connection request will formulate its own connection request **228** to the CE3 element as:

[0145] Connection request:

Source address=10.1.1.1,

Destination address=10.1.1.3,

GID=45678

[0146] The connection is then terminated upon the CE3 **229** as desired in the original connection request.

[0147] **Glossary of Acronyms Used**

AD - Virtual Private Network Auto-Discovery

BGP – Border Gateway Protocol (an inter-autonomous system routing protocol)

BGP-MP – BGP Multi-protocol Extensions

CPI – Customer Port Identifier

GID – Globally Unique Identifier

GIT – Globally Unique Identifier Table

GVPN – Generalized VPN (a port-based Optical VPN service)

HOVPN – Hierarchical Optical VPNs

HPIT – PIT Hierarchy Tree

PIT – Port Information Table

PPI – Provider Port Identifier

RPIT – Root PIT

TNA – Transport Network Assigned Address

VPOXC – Virtual private Optical cross-Connect (a port-based VPN service).

VPSTN – Virtual Private Switched Transport Network (a partition-based VPN service)

[0148] While the invention has been described in conjunction with specific embodiments thereof, it is evident that many alternatives, modifications, and variations will be apparent to those skilled in the art in light of the foregoing description. Accordingly, it is intended to embrace all such alternatives, modifications, and variations as fall within the spirit and broad scope of the appended claims.